AMENDMENTS TO THE SPECIFICATION

Please amend the following paragraphs in the specification:

Please amend the paragraph beginning on page 26, line 20 with the following amended paragraph:

FIGs. 21A-C are ~~is a~~ schematic views ~~with subfigures~~ for explaining a typical signature process performed by signature modules (as example 1);

Please amend the paragraph beginning on page 26, line 23 with the following amended paragraph.

FIGs. 22A-C are ~~is a~~ schematic views ~~with subfigures~~ for explaining another typical signature process performed by signature modules (as example 2);

Please amend the paragraph beginning on page 27, line 2 with the following amended paragraph.

FIGs. 23A-C are ~~is a~~ schematic views ~~with subfigures~~ for explaining another typical signature process performed by signature modules (as example 3);

Please amend the papagraph beginning on page 27, line 5 with the following amended paragraph.

FIGs. 24A-D are ~~is a~~ schematic views ~~with subfigures~~ for explaining another typical signature process performed by signature modules (as example 4);

Please amend the paragraph beginning on page 60, line 7 with the following amended paragraph.

If the check in step S253 reveals that the requesting registration authority is not subject to load distribution, step S254 is reached. In step S254, a check is made by referencing the RA management database (FIG. 11) to see whether the registration authority in question corresponds to multiple signature algorithms. If in step S254 the registration authority is judged corresponding to multiple signature algorithms, step S255 is reached. In step S255, a search is made through the RA management database for data entries corresponding to the requested

signature algorithms in the public key certificate issuance request. If relevant data entries are found in step S256, HSM identifiers associated with the RA identifier are acquired in step S257 from the database, and the HSMs having the obtained HSM identifiers are determined as the signature modules.

Please amend the paragraph beginning on page 62, line 2 with the following amended paragraph.

FIGs. 21A-C illustrates a typical configuration including an end entity (EE) 300, registration authorities (RA) 311 and 312, a certificate authority (CA) server 321; and HSMs 331, 332 and 333 having a signature module each. The end entity 300 issues a public key certificate issuance request to the CA server 321 through the registration authority 311 or 312.

Please amend the paragraph beginning on page 62, line 9 with the following amended paragraph. For the above setup, it is assumed that the RA management database of the CA server contains data such as those shown in ~~subfigure (a) of~~ FIG. 21B and that the verification key database accommodates data listed illustratively in ~~subfigure (b) of~~ FIG. 21C. As evident from the RA management database entries in subfigure (a), the registration authority 311 identified as RA1 allows a signature module HSM1 to execute a signature based on the RSA signature algorithm with a key length of 1,024 bits. The registration authority 312 identified as RA2 permits signature execution based on multiple algorithms: RSA signature algorithm with a key length of 2,048 bits, ECDSA with a key length of 192 bits and a parameter p=xx . . . , and ECDSA with a key length of 192 bits and a parameter p=yy . . . For the registration authority RA2, RSA signature is executed by a signature module HSM2 and ECDSA signature by a signature module HSM3. The verification key database contains signature algorithms, key lengths, parameter information, and verification keys corresponding to the HSMs configured.

Please amend the paragraph beginning on page 63, line 10 with the following amended paragraph.

FIGs. 22A-C shows an example in which the end entity (EE) 300 outputs a public key certificate issuance request to the registration authority (RA1) 311. Numerals (1) through (10) in FIG. 22A represent steps to be taken by the parties involved. These steps are described below in ascending order.

Please amend the paragraph beginning on page 64, line 5 with the following amended paragraph.

(4) Upon receipt of the certificate issuance request, the CA server 321 references the RA management database to determine an HSM for signature execution. In this example, a module HSM1 is selected as the signature execution module in accordance with the RA management database entries shown in ~~subfigure (a) of~~ FIG. 21B.

Please amend the paragraph beginning on page 64, line 11 with the following amended paragraph.

(5) The CA server 321 outputs a signature generation instruction to the signature module (HSM1) 331. The instruction, as shown in ~~subfigure (b) of~~ FIG. 22C, contains a signature generation instruction command and message data for a certificate to be generated. If the module HSM1 is capable of generating variable length keys, the signature generation instruction may include data for specifying a key length.

Please amend the paragraph beginning on page 65, line 11 with the following amended paragraph.

FIGs. 23A-C shows another example in which the end entity (EE) 300 outputs a public key certificate issuance request to the registration authority (RA2) 312. Numerals (1) through (10) in FIG. 23A represent steps to be taken by the parties involved. These steps are described below in ascending order.

Please amend the paragraph beginning on page 66, line 1 with the following amended paragraph.

(3) The registration authority 312 then transmits the certificate issuance request to the CA server 321, along with a certificate issuance request command, necessary message data including certificate storage data, a registration authority identifier (ID); and data specifying a signature algorithm, a key length and parameters, as shown in ~~subfigure (a) of~~ FIG. 23B.

Please amend the paragraph beginning on page 66, line 8 with the following amended paragraph.

(4) Upon receipt of the certificate issuance request, the CA server 321 references the RA management database to determine an HSM for signature execution. In this example, a module HSM3 is selected as the signature execution module in accordance with the RA management database entries shown in ~~subfigure (a) of~~ FIG. 21B.

Please amend the paragraph beginning on page 66, line14 with the following amended paragraph.

(5) The CA server 321 outputs a signature generation instruction to the signature module (HSM3) 333. The instruction, as shown in ~~subfigure (b) of~~ FIG. 23C, contains a signature generation instruction command, message data for a certificate to be generated, and data designating the key length and parameters.

Please amend the parargraph beginning on page 67, line11 with the following amended paragraph.

FIGs. 24A-D shows yet another example in which the end entity (EE) 300 outputs a public key certificate issuance request to the registration authority (RA2) 312, soliciting simultaneous execution of a plurality of signatures. Numerals (1) through (14) in FIG. 24 denote steps to be taken by the parties involved. These steps are described below in ascending order.

Please amend the paragraph beginning on page 68, line 3 with the following amended paragraph.

(3) The registration authority 312 then transmits the certificate issuance request to the CA server 321, along with a certificate issuance request command, necessary message data including certificate storage data, a registration authority identifier (ID); and data specifying a plurality of signature algorithms, key lengths and parameters, as shown in ~~subfigure (a) of~~ FIG. 24B.

Please amend the paragraph beginning on page 68, line 11 with the following amended paragraph.

(4) Upon receipt of the certificate issuance request, the CA server 321 references the RA management database to determine HSMs for signature execution. In this example, modules HSM 2 and HSM3 are selected as the signature execution modules in accordance with the RA management database entries shown in ~~subfigure (a) of~~ FIG. 21B.

Please amend the paragraph beginning on page 68, line 17 with the following amended paragraph.

(5) The CA server 321 outputs a signature generation instruction first to the signature module (HSM2) 332. The instruction, as shown in ~~subfigure (b) of~~ FIG. 24C, contains a signature generation instruction command, message data for a certificate to be generated, and data designating a key length.

Please amend the paragraph beginning on page 69, line 9 with the following amended paragraph.

(9) The CA server 321 then outputs the signature generation instruction to the signature module (HSM3) 333. The instruction, as shown in ~~subfigure (c) of~~ FIG. 24D, contains a signature generation instruction command, message data for a certificate to be generated, and data designating the key length and parameters.